

luckycloud GmbH

Security Vulnerability Register

Public register of known vulnerabilities affecting luckycloud cloud services — updated continuously

Last Updated	Open Critical/High	Detection Tool	Hosts Monitored
1 June 2026	0	Wazuh (CVE feed updated every 60 min)	All production hosts

This register lists known vulnerabilities that have affected luckycloud’s production infrastructure, with their CVSS severity scores, affected component, remediation responsibility, and patch status. luckycloud GmbH operates the full cloud platform and is responsible for patching all infrastructure and application-level components. Customers do not deploy software on the platform directly.

Current Status — Open Vulnerabilities

■ No open Critical or High vulnerabilities

All critical and high severity findings identified during the current period have been remediated. Vulnerability detection runs continuously via Wazuh across all production hosts.

Remediated Findings — Attestation Period 2026

CVE ID	CVE Name	CVSS	Severity	Affected Component	Responsibility	Debian Patch Date	Status	luckycloud Patched
CVE-2026-31431	Copy Fail	7.8	High	Linux kernel (algif_aead)	CSP	5 May 2026	Patched	5 May 2026
CVE-2026-43284	Dirty Frag	7.8	High	Linux kernel (xfrm ESP)	CSP	16 May 2026	Patched	16 May 2026
CVE-2026-43500	Dirty Frag	7.8	High	Linux kernel (RxRPC)	CSP	16 May 2026	Patched	16 May 2026

CVE-2026-31431 (Copy Fail) was disclosed 29 April 2026; Debian released the security patch on 5 May 2026 and luckycloud applied it the same day. CVE-2026-43284 and CVE-2026-43500 (Dirty Frag) were disclosed 7–8 May 2026; both were included in Debian 12.14 released on 16 May 2026 and luckycloud applied them the same day.

Patch Response Timelines

Severity	CVSS Score	Maximum Time to Patch
Critical	9.0 or above	72 hours
High	7.0 – 8.9	14 days
Medium	4.0 – 6.9	30 days
Low	Below 4.0	Next scheduled maintenance window

Remediation Responsibility

Component Type	Responsible Party	Description
Infrastructure and OS	CSP (luckycloud)	luckycloud is responsible for patching all server-level components and operating system packages.
Applications and services	CSP (luckycloud)	luckycloud operates and maintains all applications and services on the platform. Customers do not deploy software directly.
Platform configuration (TLS, encryption, access)	CSP (luckycloud)	luckycloud manages all platform-level configuration including TLS certificates, encryption at rest, and access controls.

For security enquiries: security@luckycloud.de

luckycloud GmbH — luckycloud.de — Last updated 1 June 2026